

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

2037 Pembroke Forest Drive,
Winston-Salem, North Carolina 27106

Case No. 1:17-mi-00224-1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The premises located at 2037 Pembroke Forest Drive, Winston-Salem, NC, 27106, more particularly described in Attachment A, attached hereto and made part hereof.

located in the Middle District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

Evidence of, instrumentalities used in committing, and fruits of the crime of 18 U.S.C. § 875(c), all of which are more particularly described in Attachment B, attached hereto and made a part hereof.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 875(c)

Offense Description
Transmitting/Communicating a Threat in Interstate or Foreign Commerce

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Lawrence O. Anyaso, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/29/17 2:55pm

City and state: Durham, North Carolina


Judge's signature

Honorable Joe L. Webster, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Lawrence o. Anyaso, a Special Agent with the United States Capitol Police, being duly sworn, depose and state as follows:

AFFIANT

1. I am with the United States Capitol Police (the "USCP"), where I have served since June 13, 2003. I am currently assigned to the Investigations Division, Threat Assessment Section. I have attended the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia, and the USCP three-week Crime Scene Investigation course. In the course of my employment as a Special Agent with the USCP, I have received training regarding the application for and execution of both search and arrest warrants. In my current assignment, I have been involved in numerous cases involving harassing and threatening communications, both locally and interstate.

2. I have participated in numerous investigations into threats against members of Congress to include violations of Title 18, U.S.C. § Section 875(C), which provides:

Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of a criminal investigation involving **Timothy George DOWD (hereinafter, DOWD)** for threatening to assassinate Members of Congress, in violation of Title 18, U.S.C. § 875(C)

4. The facts and information contained in this affidavit are based upon my training and experience, participation in threats investigations, personal knowledge, and observations during the course of this investigation, as well as the observations of other agents involved in this investigation. All observations not personally made by me were related to me by the individuals who made them or were conveyed to me by my review of records, documents, and other physical evidence obtained during the course of this investigation. This affidavit contains information necessary to support probable cause and is not intended to include each and every fact and matter observed by me or known to the Government.

SOURCES OF INFORMATION

The statements in this affidavit are based on information provided to me by other USCP agents and Federal Bureau of Investigation agents, local law enforcement officers, as well as my own investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

PROBABLE CAUSE

1. On Friday, June 23, 2017 at approximately 2:27pm, DOWD sent an email to the USCP Public Information Office (PIO) in Washington, DC. The email was sent from the email address, Timonthy.Dowd7@gmail.com with the subject line: "Target and assassinate Congress swine."

2. The email contained the following threatening statement:

"Plenty of us who hate the government filth that is ruining this country. I myself am coordinating and planning assassinations against the sub-human members of Congress. I just hate them and want them to die." Timothy Dowd

3. The USCP is the law enforcement agency in the legislative branch responsible for the protection of Members of Congress and the investigation of crimes against Members of Congress to include threats.

4. Witness 1, an employee in the USCP PIO office, reviewed the message and contacted the USCP Investigation Division- Threat Assessment Section (TAS) to report the threat for investigation.

5. Business subscriber records, provided by Google, revealed the Internet Protocol (IP) address, 2606:a000:898f:9800:d150:4d64:7491:def2, as being accessed by the email address, Timothy.Dowd7@gmail.com to send the email. Google also provided the subscribers name as Timothy Dowd and the phone number, 704-456-XXXX which was connected to DOWD through an open source search and law enforcement databases.

6. An open source search of the IP address revealed the address to resolves to Time Warner Cable with a Geo-location of Winston-Salem, North Carolina which is in the Middle District of North Carolina.

7. Time Warner Cable provided subscriber account information for the IP address 2606:a000:898f:9800:d150:4d64:7491:def2 which was accessed on June 23, 2017 at 2:27pm. Time Warner Cable identified the subscriber as William F. Dowd Jr. with a billing address of 2037 Pembroke Forest Dr. Winston-Salem, NC and a phone number, 704-763-XXXX.

8. An open source search of the subscriber address, using the website Accurint, identified William and Geraldine Dowd as the owners of the residence. Timothy DOWD was listed as being a resident of this address.

9. A check of law enforcement databases, revealed that DOWD has a history of making threats to US. Government officials.

10. On June 28, 2017, FBI Special Agent conducted spot-check surveillance of 2037 Pembroke Forest Drive, Winston-Salem, NC, 27106. At approximately 7:48am, SA Spainhour observed a 2010 Chevrolet Corvette, bearing North Carolina License Plate: CAR-8142, Gray in color, leaving the area of the residence on Pembroke Forest Drive. The Corvette appeared to be driven by Timothy George Dowd. SA Spainhour followed the Corvette for several minutes and took a photograph of the vehicle at the intersection of University Parkway and Home Road, in Winston-Salem, NC.

TECHNICAL TERMS

1. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal

computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

- c. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- d. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- e. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- f. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer

attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- h. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

2. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

3. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will

be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

4. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware,

and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

5. *Necessity of seizing or copying entire computers or storage media.*

In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image

copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction.

This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

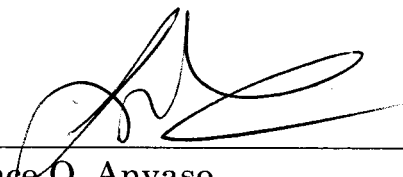
6. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

7. Because at least two people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION


8. Based on upon the foregoing, Your Affiant submits there is probable cause to believe that on or about June 23, 2017, DOWD threatened to assassinate Members of Congress in violation of Title 18, United States Code, § 875(C).

WHEREFORE, your Affiant submits that this Affidavit supports probable cause for a warrant to search the residence located at 2037 Pembroke Forest Drive, Winston-Salem, NC, 27106, the vehicle A 2010 Chevrolet Corvette, VIN: 1G1YE2DW1A5109417, North Carolina License Plate: CAR-8142, Gray in color, registered to Timothy George Dowd, and the person of Timothy George Dowd, White/Male, DOB: 09/12/1986, for evidence related to the threats made against Members of Congress in violation of 18 U.S.C. § 875(C).



Lawrence O. Anyaso
Special Agent
United States Capitol Police

Sworn and subscribed before me this _____ day of June 2017.



THE HONORABLE JOE L. WEBSTER
UNITED STATES MAGISTRATE JUDGE

2:55 pm

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire premises, including any outbuildings, located at 2037 Pembroke Forest Drive, Winston-Salem, NC, 27106. The residence is described as a two story single family residence with basement, two car garage, with white siding, dark colored shutters, and red brick foundation. The residence driveway is on the left side of the property when facing the front of the residence. A black mailbox displaying the numbers “2037” is located at the end of the residence driveway, where it meets Pembroke Forest Drive. The Forsyth County Tax Office lists the residence as PIN# 6818-48-3001, Property Description LO045 B L3491D.





ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 875 (c).

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;

- e. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - f. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - g. evidence of the times the COMPUTER was used;
 - h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - j. records of or information about Internet Protocol addresses used by the COMPUTER;
 - k. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses related to threats made against Members of Congress and
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
 - 4. Any cameras, video cameras, cell phones, tablets, or other digital media capable of creating video, images, or screenshots of threats against the government, to include the United States Congress.
 - 5. Records, information, and items relating to violations of the statutes described above in the form of:

- a. Records, information, and items referencing or revealing the occupancy or ownership of 2037 Pembroke Forest Drive, Winston-Salem, North Carolina, 27106, including utility and telephone bills, mail envelopes, or addressed correspondence;
- b. Records, information, and items referencing or revealing the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
- c. Records and information referencing or revealing the identity of any individual using online moniker or email address "timothy.dowd7@gmail.com"
- d. Records and information revealing the use and identification of remote computing services such as email accounts or cloud storage;
- e. Records related to any threats made against the United States Government, to include the Members of Congress;

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD Cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

ATTACHMENT C

DESCRIPTION OF VEHICLE TO BE SEARCHED

A 2010 Chevrolet Corvette, VIN: 1G1YE2DW1A5109417, North Carolina License Plate: CAR-8142, Gray in color, registered to Timothy George Dowd, White/Male, DOB: 09/12/1986, 511 N. Main Street, Mount Gilead, NC, 27306.



ATTACHMENT D

DESCRIPTION OF PERSON TO BE SEARCHED

Timothy George Dowd, White/Male, DOB: 09/12/1986, NCDL# 23877455, 2037 Pembroke Forest Drive, Winston-Salem, NC, 27106

